

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-110628

(43)Date of publication of application : 11.04.2003

(51)Int.Cl.

H04L 12/66

H04L 9/08

H04L 9/32

H04L 12/56

(21)Application number : 2001-300137

(71)Applicant : NEC CORP

(22)Date of filing : 28.09.2001

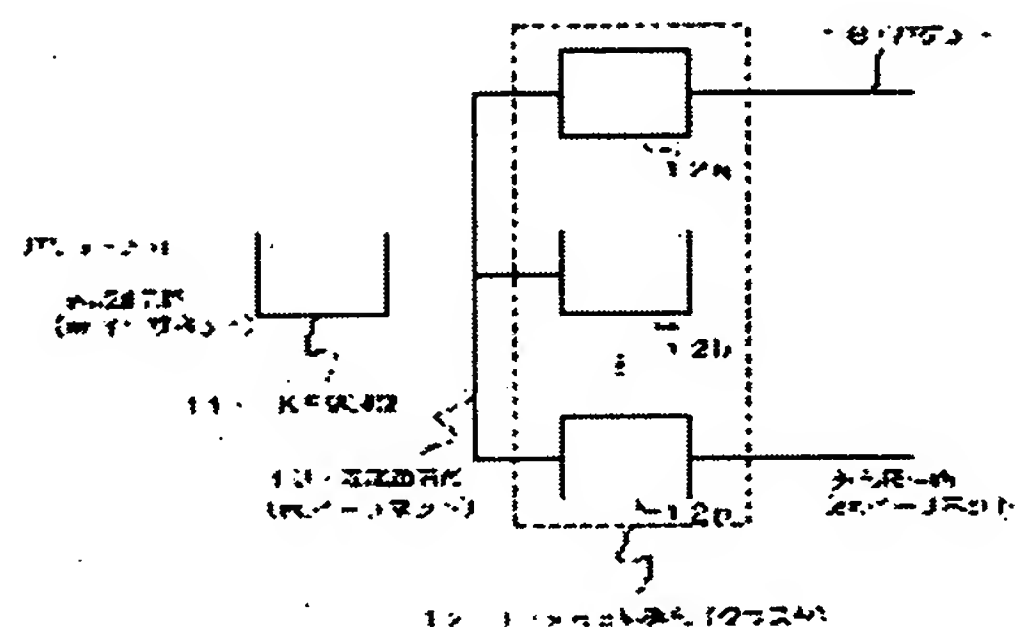
(72)Inventor : KUBO TAKUYA

(54) SECURITY GATEWAY APPARATUS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a security gateway apparatus in a system for communicating encrypted packets that can prevent loads of arithmetic processing required for encrypting the packets from being concentrated so as to relieve the load for arithmetic processing in respective components.

SOLUTION: The security gateway apparatus comprises; an authentication key exchange means 11 for conducting negotiation processing to negotiate parameters required for IP security communication with an opposed security gateway; and an IP security processing means 12 connected to the authentication key exchange means 11 via an internal communication path 13 and executing IP security processing for a packet sent from the authentication key exchange means 11.



LEGAL STATUS

[Date of request for examination]

13.08.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3603830

[Date of registration]

08.10.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P) (12) 公開特許公報 (A) (11) 特許出願公開番号
特開2003-110628
(P2003-110628A)
(43) 公開日 平成15年4月11日 (2003.4.11)

(51) Int.Cl.⁷ 識別記号 F I テーマコード^{*}(参考)
H 0 4 L 12/66 H 0 4 L 12/66 B 5 J 1 0 4
9/08 12/56 H 5 K 0 3 0
9/32 9/00 6 0 1 C
12/56 6 7 5 A

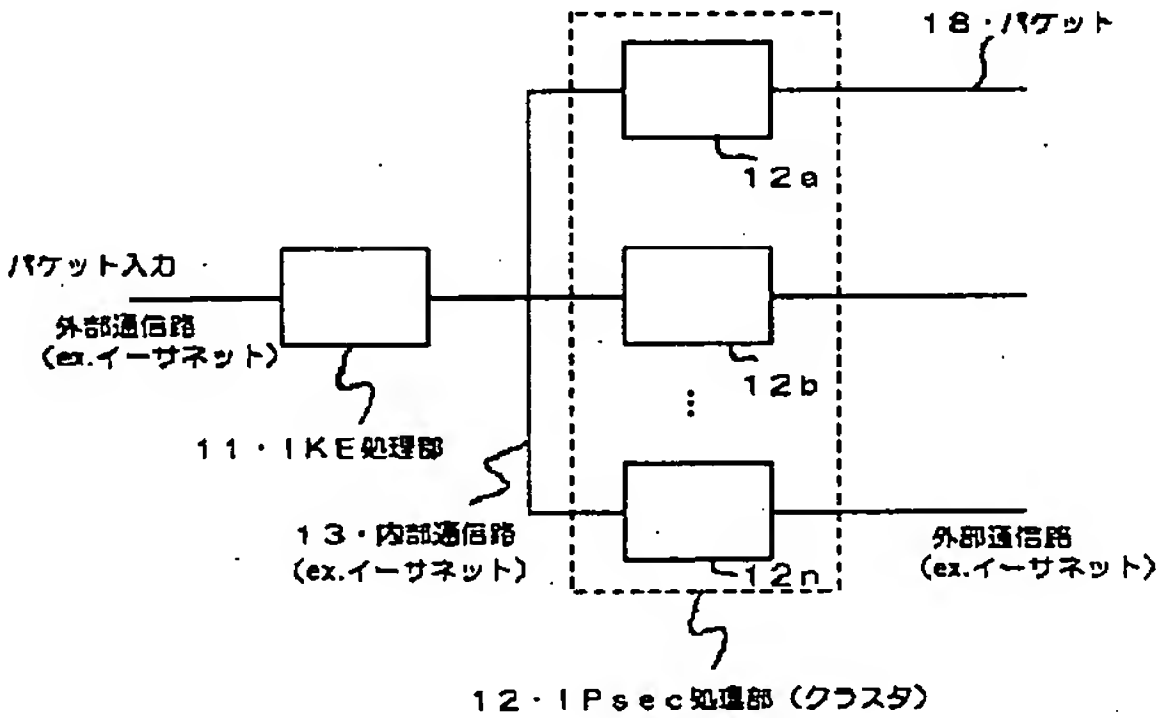
審査請求 有 請求項の数21 O L (全 10 頁)

(21) 出願番号 特願2001-300137(P2001-300137)
(22) 出願日 平成13年9月28日 (2001.9.28)

(71) 出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号
(72) 発明者 久保 拓也
東京都港区芝五丁目7番1号 日本電気株式会社内
(74) 代理人 100096105
弁理士 天野 広
Fターム(参考) 5J104 AA01 AA16 EA04 EA26 NA02
NA05 PA07
5K030 GA15 HA08 HB18 HD03 HD08
KA07 LE03

(54) 【発明の名称】 セキュリティゲートウェイ装置

(57) 【要約】
【課題】 パケットを暗号化して通信を行うシステムにおいて、パケットの暗号化に要する演算処理の負荷の集中を防止し、個々のコンポーネントにおける演算処理の負荷を減少させる。
【解決手段】 本セキュリティゲートウェイ装置は、IPセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートするネゴシエーション処理を行う認証キー交換手段11と、認証キー交換手段11と内部通信路13で接続されており、認証キー交換手段11から送られてきたパケットに対してIPセキュリティ処理を実行するIPセキュリティ処理手段12と、からなる。



【特許請求の範囲】

【請求項1】 IPセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートするネゴシエーション処理を行う認証キー交換手段と、

前記認証キー交換手段と内部通信路で接続されており、前記認証キー交換手段から送られてきたパケットに対してIPセキュリティ処理を実行するIPセキュリティ処理手段と、

からなるセキュリティゲートウェイ装置。

【請求項2】 前記IPセキュリティ処理手段は複数のIPセキュリティ処理装置からなり、前記認証キー交換手段は、前記ネゴシエーション処理後に、前記パケットを前記複数のIPセキュリティ処理装置の何れかに振り分ける振り分け処理を行い、前記複数のIPセキュリティ処理装置の各々は前記認証キー交換手段から振り分けられた前記パケットに対してIPセキュリティ処理を実行するものであることを特徴とする請求項1に記載のセキュリティゲートウェイ装置。

【請求項3】 前記認証キー交換手段は、IPセキュリティ処理を行うべきパケットを受信した場合には、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットのIPセキュリティ処理を行うIPセキュリティ処理装置を決定し、前記パケットを前記IPセキュリティ処理装置に転送することを特徴とする請求項2に記載のセキュリティゲートウェイ装置。

【請求項4】 前記認証キー交換手段はローカルデータベースを有しており、前記認証キー交換手段は、検索したパラメータと、前記パケットのIPセキュリティ処理を行わせることに決定した前記IPセキュリティ処理装置の識別子とを相互にリンク付けした状態で、前記パラメータ及び前記識別子を前記ローカルデータベースに保存することを特徴とする請求項3に記載のセキュリティゲートウェイ装置。

【請求項5】 前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記IPセキュリティ処理装置に転送することを特徴とする請求項3または4に記載のセキュリティゲートウェイ装置。

【請求項6】 前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えており、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存するものであることを特徴とする請求項2乃至5の何れか一項に記載のセキュリティゲートウェイ装置。

【請求項7】 前記認証キー交換手段から前記パケットを受信した前記IPセキュリティ処理装置は、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パ

ケットに対してIPセキュリティ処理を行うことを特徴とする請求項6に記載のセキュリティゲートウェイ装置。

【請求項8】 前記認証キー交換手段は前記パケットをカプセル化し、カプセル化した前記パケットを前記IPセキュリティ処理装置に転送することを特徴とする請求項3に記載のセキュリティゲートウェイ装置。

【請求項9】 前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えており、

10 前記複数のIPセキュリティ処理装置の各々は、前記認証キー交換手段から受信したカプセル化した前記パケットを復元し、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してIPセキュリティ処理を行うことを特徴とする請求項8に記載のセキュリティゲートウェイ装置。

【請求項10】 前記認証キー交換手段並びに前記複数のIPセキュリティ処理装置の各々はプロセッサを搭載した基板から構成されており、前記認証キー交換手段並びに前記複数のIPセキュリティ処理装置の各々は内部バスで相互に接続されていることを特徴とする請求項1乃至9の何れか一項に記載のセキュリティゲートウェイ装置。

【請求項11】 前記認証キー交換手段と前記IPセキュリティ処理手段との間におけるパケットの転送は、データリンクレイヤの種別に応じて、最適化されることを特徴とする請求項1乃至10の何れか一項に記載のセキュリティゲートウェイ装置。

【請求項12】 認証キー交換手段が、IPセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートする第1の過程と、前記認証キー交換手段と内部通信路で接続されているIPセキュリティ処理手段において、前記認証キー交換手段から送られてきたパケットに対してIPセキュリティ処理を実行する第2の過程と、からなるパケットに対するIPセキュリティ処理方法。

【請求項13】 前記IPセキュリティ処理手段は複数のIPセキュリティ処理装置からなり、前記第1の過程の後に、前記認証キー交換手段が、前記パケットを前記複数のIPセキュリティ処理装置の何れかに振り分ける第3の過程をさらに備え、前記第2の過程においては、前記複数のIPセキュリティ処理装置の各々が前記認証キー交換手段から振り分けられた前記パケットに対してIPセキュリティ処理を実行するものであることを特徴とする請求項12に記載のパケットに対するIPセキュリティ処理方法。

【請求項14】 前記認証キー交換手段が、IPセキュリティ処理を行うべきパケットを受信した場合には、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索する第4の過程と、

検索したパラメータに基づいて、前記バケットのIPセキュリティ処理を行うIPセキュリティ処理装置を決定する第5の過程と、

前記バケットを前記第5の過程において決定した前記IPセキュリティ処理装置に転送する第6の過程と、
を備えることを特徴とする請求項13に記載のバケットに対するIPセキュリティ処理方法。

【請求項15】 前記認証キー交換手段はローカルデータベースを有しており、
前記認証キー交換手段が、検索したパラメータと、前記バケットのIPセキュリティ処理を行わせることに決定した前記IPセキュリティ処理装置の識別子とを相互にリンク付けする過程と、

前記認証キー交換手段が、前記パラメータ及び前記識別子を前記ローカルデータベースに保存する過程と、
を備えることを特徴とする請求項14に記載のバケットに対するIPセキュリティ処理方法。

【請求項16】 前記第6の過程において、前記認証キー交換手段は、検索したパラメータを前記バケットとともに前記IPセキュリティ処理装置に転送することを特徴とする請求項14または15に記載のバケットに対するIPセキュリティ処理方法。

【請求項17】 前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えており、
前記複数のIPセキュリティ処理装置の各々が、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存する過程を備えることを特徴とする請求項13乃至16の何れか一項に記載のバケットに対するIPセキュリティ処理方法。

【請求項18】 前記認証キー交換手段から前記バケットを受信した前記IPセキュリティ処理装置が、前記ローカルデータベースから、前記バケットに対応するパラメータを検索する過程と、

前記IPセキュリティ処理装置が、検索したパラメータに基づいて、前記バケットに対してIPセキュリティ処理を行う過程と、

を備えることを特徴とする請求項17に記載のバケットに対するIPセキュリティ処理方法。

【請求項19】 前記認証キー交換手段が前記バケットをカプセル化する過程を備えており、
前記カプセル化された前記バケットが前記第6の過程において前記IPセキュリティ処理装置に転送されることを特徴とする請求項14に記載のバケットに対するIPセキュリティ処理方法。

【請求項20】 前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えており、
前記複数のIPセキュリティ処理装置の各々が、前記認証キー交換手段から受信したカプセル化した前記バケットを復元する過程と、

前記複数のIPセキュリティ処理装置の各々が、前記ロ

ーカルデータベースから、前記バケットに対応するパラメータを検索する過程と、

前記複数のIPセキュリティ処理装置の各々が、検索したパラメータに基づいて、前記バケットに対してIPセキュリティ処理を行う過程と、

を備えることを特徴とする請求項19に記載のバケットに対するIPセキュリティ処理方法。

【請求項21】 前記認証キー交換手段と前記IPセキュリティ処理手段との間におけるバケットの転送を、データリンクレイヤの種別に応じて、最適化する過程を備えることを特徴とする請求項12乃至20の何れか一項に記載のバケットに対するIPセキュリティ処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、イントラネットとインターネットとを接続するために使用されるゲートウェイ装置におけるセキュリティを向上させたセキュリティゲートウェイ装置に関する。

【0002】

【従来の技術】インターネットのアプリケーションの一つとして、仮想専用線(Virtual Private Network:VPN)がある。この仮想専用線においては、インターネット自体のオープン性から、セキュリティの問題があるため、インターネットプロトコル(IP)にセキュリティ機能を付加するプロトコルであるIPセキュリティ(IP Security:以下「IPsec」と記す)によりバケットを暗号化して通信を行うことが必須となっている。

【0003】図9は従来の信号通信システムの一例のブロック図である。

【0004】この暗号通信システムにおいては、端末100a-100nからなる第1のグループの各端末に第1の暗号ゲートウェイ装置110が接続されており、同様に、端末120a-120nからなる第2のグループの各端末に第2の暗号ゲートウェイ装置130が接続されている。第1の暗号ゲートウェイ装置110と第2の暗号ゲートウェイ装置130とはネットワーク140を介して相互に接続されている。

【0005】第1のグループの各端末100a-100nと第2のグループの各端末120a-120nとの間の通信において、第1及び第2の暗号ゲートウェイ装置110、130を介して通信されるバケットデータの暗号化アルゴリズムあるいは暗号化に使用する鍵その他のパラメータは、第1及び第2の暗号ゲートウェイ装置110、130間においては、固定されている。

【0006】図9に示すような暗号通信システムにおいては、第1及び第2の暗号ゲートウェイ装置110、130を通過しないバケットは、本来、復号化されることはない。しかしながら、第1及び第2の暗号ゲートウェイ装置110、130を接続するネットワーク140に

においては、これらの暗号化されたパケットが傍受され、パケットの暗号化アルゴリズムや鍵を解読されるおそれがある。

【0007】このようなおそれに対して、例えば、特開平7-107082号公報は、暗号化または非暗号化の選択またはセッション鍵の選択を端末の組み合わせ毎に、あるいは、セッション毎に設定することができる暗号ゲートウェイ装置を開示している。

【0008】

【発明が解決しようとする課題】また、RFC (Request For Comments) 1825-1828には、インターネットプロトコル(IP)におけるセキュリティを扱った「Security Architecture for Internet Protocol」(以下「IPsec」と呼ぶ)が規定されている。

【0009】図10は、IPsecにおいて規定されているIP用セキュリティ認証ヘッダの一例を示す図である。

【0010】このIP用セキュリティ認証ヘッダには、このヘッダの次のヘッダの識別子、このヘッダの長さ、SPI (Security Parameter Index) 可変長の認証データ(authenticated data)が格納されている。このIP用セキュリティ認証ヘッダは、各IPパケットにおいて、IPヘッダとIPデータグラムとの間に挿入される。

【0011】上述したようなパケットの暗号化処理はそれ自体非常に演算処理負荷が高い。このため、専用の暗号LSIを適用するなどの性能向上がはかられているが、根本的な解決にはなっていないのが現状である。

【0012】本発明は、このような問題点に鑑みてなされたものであり、パケットを暗号化して通信を行うシステムにおいて、パケットの暗号化に要する演算処理の負荷の集中を防止し、個々のコンポーネントにおける演算処理の負荷を減少させることを可能にするセキュリティゲートウェイ装置及びパケット処理方法を提供することを目的とする。

【0013】

【課題を解決するための手段】この目的を達成するため、本発明は、IPセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートするネゴシエーション処理を行う認証キー交換手段と、前記認証キー交換手段と内部通信路で接続されており、前記認証キー交換手段から送られてきたパケットに対してIPセキュリティ処理を実行するIPセキュリティ処理手段と、からなるセキュリティゲートウェイ装置を提供する。

【0014】前記IPセキュリティ処理手段は複数のIPセキュリティ処理装置からなるものとすることができる。この場合、前記認証キー交換手段は、前記ネゴシエ

ーション処理後に、前記パケットを前記複数のIPセキュリティ処理装置の何れかに振り分ける振り分け処理を行い、前記複数のIPセキュリティ処理装置の各々は前記認証キー交換手段から振り分けられた前記パケットに対してIPセキュリティ処理を実行する。

【0015】本発明に係るセキュリティゲートウェイ装置においては、IPsec通信に必要な2つの機能要素である認証キー交換(Internet Key Exchange: IKE)とIPsecとが別手段として配備され、さらに、IPsec通信のバンドルが負荷分散される。これにより、通信スループットをマクロレベルで向上させることが可能となる。

【0016】さらに、IPセキュリティ処理手段をクラスタ構成とし、すなわち、複数のIPセキュリティ処理装置からなるものとするにより、セキュリティゲートウェイ装置全体のスケーラビリティを確保することが可能となる。

【0017】前記認証キー交換手段は、IPセキュリティ処理を行うべきパケットを受信した場合には、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットのIPセキュリティ処理を行うIPセキュリティ処理装置を決定し、前記パケットを前記IPセキュリティ処理装置に転送するものとして構成することができる。

【0018】前記認証キー交換手段はローカルデータベースを有しているものとして構成することができる。この場合、前記認証キー交換手段は、検索したパラメータと、前記パケットのIPセキュリティ処理を行わせることに決定した前記IPセキュリティ処理装置の識別子とを相互にリンク付けした状態で、前記パラメータ及び前記識別子を前記ローカルデータベースに保存することができる。

【0019】前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記IPセキュリティ処理装置に転送することが好ましい。

【0020】前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えており、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存するものとして構成することができる。

【0021】前記認証キー交換手段から前記パケットを受信した前記IPセキュリティ処理装置は、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してIPセキュリティ処理を行うものとして構成することができる。

【0022】前記認証キー交換手段は前記パケットをカプセル化し、カプセル化した前記パケットを前記IPセキュリティ処理装置に転送するものとして構成すること

ができる。

【0023】前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えているものとして構成することができる。この場合、前記複数のIPセキュリティ処理装置の各々は、前記認証キー交換手段から受信したカプセル化した前記パケットを復元し、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してIPセキュリティ処理を行うことものとして構成することができる。

【0024】前記認証キー交換手段並びに前記複数のIPセキュリティ処理装置の各々はプロセッサを搭載した基板から構成することができる。この場合、前記認証キー交換手段並びに前記複数のIPセキュリティ処理装置の各々は内部バスで相互に接続される。

【0025】前記認証キー交換手段と前記IPセキュリティ処理手段との間におけるパケットの転送は、データリンクレイヤの種別に応じて、最適化することが可能である。

【0026】また、本発明は、認証キー交換手段が、IPセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートする第1の過程と、前記認証キー交換手段と内部通信路で接続されているIPセキュリティ処理手段において、前記認証キー交換手段から送られてきたパケットに対してIPセキュリティ処理を実行する第2の過程と、からなるパケットに対するIPセキュリティ処理方法を提供する。

【0027】前記IPセキュリティ処理手段は複数のIPセキュリティ処理装置からなるものとして構成することができる。この場合、本方法は、前記第1の過程の後、前記認証キー交換手段が、前記パケットを前記複数のIPセキュリティ処理装置の何れかに振り分ける第3の過程をさらに備え、前記第2の過程においては、前記複数のIPセキュリティ処理装置の各々が前記認証キー交換手段から振り分けられた前記パケットに対してIPセキュリティ処理を実行するものとして構成することができる。

【0028】本方法は、前記認証キー交換手段が、IPセキュリティ処理を行うべきパケットを受信した場合に、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索する第4の過程と、検索したパラメータに基づいて、前記パケットのIPセキュリティ処理を行うIPセキュリティ処理装置を決定する第5の過程と、前記パケットを前記第5の過程において決定した前記IPセキュリティ処理装置に転送する第6の過程と、を備えるものとして構成することができる。

【0029】前記認証キー交換手段はローカルデータベースを有するものとして構成することができる。この場合、本方法は、前記認証キー交換手段が、検索したパラメータと、前記パケットのIPセキュリティ処理を行わ

せることに決定した前記IPセキュリティ処理装置の識別子とを相互にリンク付けする過程と、前記認証キー交換手段が、前記パラメータ及び前記識別子を前記ローカルデータベースに保存する過程と、を備えることが好ましい。

【0030】前記第6の過程において、前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記IPセキュリティ処理装置に転送することが好ましい。

10 【0031】前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えているものとして構成することができる。この場合、本方法は、前記複数のIPセキュリティ処理装置の各々が、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存する過程を備えることができる。

20 【0032】本方法は、前記認証キー交換手段から前記パケットを受信した前記IPセキュリティ処理装置が、前記ローカルデータベースから、前記パケットに対応するパラメータを検索する過程と、前記IPセキュリティ処理装置が、検索したパラメータに基づいて、前記パケットに対してIPセキュリティ処理を行う過程と、を備えることが好ましい。

【0033】本方法は、前記認証キー交換手段が前記パケットをカプセル化する過程を備えることが好ましく、この場合、前記カプセル化された前記パケットが前記第6の過程において前記IPセキュリティ処理装置に転送されることが好ましい。

30 【0034】前記複数のIPセキュリティ処理装置の各々はローカルデータベースを備えているものとして構成することができる。この場合、本方法は、前記複数のIPセキュリティ処理装置の各々が、前記認証キー交換手段から受信したカプセル化した前記パケットを復元する過程と、前記複数のIPセキュリティ処理装置の各々が、前記ローカルデータベースから、前記パケットに対応するパラメータを検索する過程と、前記複数のIPセキュリティ処理装置の各々が、検索したパラメータに基づいて、前記パケットに対してIPセキュリティ処理を行う過程と、を備えることが好ましい。

40 【0035】さらに、本方法は、前記認証キー交換手段と前記IPセキュリティ処理手段との間におけるパケットの転送を、データリンクレイヤの種別に応じて、最適化する過程を備えることができる。

【0036】

【発明の実施の形態】図1は、本発明の第1の実施形態に係るセキュリティゲートウェイ装置のブロック図である。

50 【0037】IPsec通信を行う際には、対向装置との間でアルゴリズムや鍵などのIPsec通信パラメータをネゴシエートするプロトコル(IKE)と、ネゴシエートしたパラメータを適用して実際にIPsec処理

を行うプロトコル(IPsec)とが必要となる。

【0038】このため、本実施形態に係るセキュリティゲートウェイ装置は、図1に示すように、認証キー交換を行う、すなわち、IPsec通信パラメータをネゴシエートする認証キー交換処理部11(以下、「IKE処理部11」と呼ぶ)と、実際にIPsec処理を行うIPsec処理部12の2つのコンポーネントに分割されている。

【0039】さらに、IPsec処理部12をクラスタ構成とされている。すなわち、IPsec処理部12は10 n個(nは2以上の正の整数)のIPsec処理装置12a-12nから構成されている。

【0040】IKE処理部11とIPsec処理部12とはイーサネット(登録商標)その他の内部通信路13を介して接続されている。

【0041】図2は、本実施形態に係るセキュリティゲートウェイ装置のより具体的なブロック図である。

【0042】図2に示すように、IKE処理部11は対向するセキュリティゲートウェイ(SGW)14とインターネットその他のインセキュアネットワーク17を介して20 接続されている。

【0043】また、IKE処理部11はローカルデータベース15を内蔵しており、同様に、IPsec処理部12を構成するIPsec処理装置12a-12nの各々もローカルデータベース16を内蔵している。

【0044】次いで、本実施形態に係るセキュリティゲートウェイ装置の動作の概要を以下に説明する。

【0045】IKE処理部11は、対向するセキュリティゲートウェイ14との間でIKEプロトコルによりIPsec通信パラメータをネゴシエートする。ネゴシエートしたパラメータ情報(以後「IPsec SA」と呼ぶ)を、ローカルデータベース15に保存するとともに、このIPsec処理を実際に行うIPsec処理装置をIPsec処理装置12a-12nの中から一つ決定する。例えば、IPsec処理装置12aが決定される。

【0046】次いで、IPsec SAをIPsec処理装置12aに転送する。同時に、選択したIPsec処理装置12aの識別子を、対応するIPsec SAにリンク付ける。

【0047】IKE処理部11からIPsec SAを受信したIPsec処理装置12aは、そのIPsec SAをローカルデータベース16に保存する。

【0048】IKE処理部11は、セキュリティゲートウェイ14からIPsec処理すべきパケットを受信した場合、そのパケットに対応するIPsec SAを検索する。次いで、IKE処理部11は、検索したIPsec SAに基づいて、対応するIPsec処理装置(例えば、IPsec処理装置12a)を決定し、受信パケットをIPsec処理装置12aへ転送する。

【0049】IKE処理部11からIPsec処理パケットを受信したIPsec処理装置12aは、ローカルデータベース16から、対応するIPsec SAを検索する。IPsec処理装置12aは、検索したIPsec SAに基づいて、実際のIPsec処理(暗号/復号処理及び認証処理)を実行し、処理済みのパケット18を出力する。

【0050】次いで、本実施形態に係るセキュリティゲートウェイ装置の動作をIPsec SA確立フェーズ及びIPsec通信フェーズの2つのフェーズに分けて、それぞれ図2から図7までを参照して説明する。図2は、IPsec SA確立フェーズにおける本セキュリティゲートウェイ装置の作動状態を示すブロック図、図3は、IPsec通信フェーズにおける本セキュリティゲートウェイ装置の作動状態を示すブロック図、図4は、IPsec SA確立フェーズにおけるIKE処理部11の動作を示すフローチャート、図5は、IPsec SA確立フェーズにおけるIPsec処理部12の動作を示すフローチャート、図6は、IPsec通信フェーズにおけるIKE処理部11の動作を示すフローチャート、図7は、IPsec通信フェーズにおけるIPsec処理部12の動作を示すフローチャートである。

【0051】IPsec SA確立フェーズにおいては、IKE処理部11が対向するセキュリティゲートウェイ14との間で、IKEプロトコルを用いてIPsec処理に必要な各種パラメータ(アルゴリズム、鍵等)をネゴシエートする(図4のステップS401)。以後、このネゴシエーション処理の実行をIPsec SA確立と呼ぶ。

【0052】IPsec SAを確立すると、IKE処理部11は、このIPsec処理を実際に行うIPsec処理装置として、クラスタすなわちIPsec処理装置12a-12nの中から一つのIPsec処理装置を選択する(図4のステップS402)。この際、ラウンドロビン等のアルゴリズムにより、クラスタ内の負荷分散を考慮して、IPsec処理装置を選択する。ここでは、IPsec処理装置12nが選択されたものと想定する。

【0053】次いで、IKE処理部11は、IPsec SAと選択したIPsec処理装置12nの識別子とをリンク付けし、双方をローカルデータベース15に保存する(図4のステップS403)。例えば、図2に示すように、ローカルデータベース15には、IPsec SAとしてパラメータ「SA₁₁」、それに対応するIPsec処理装置としてIPsec処理装置12nの識別子「23」がリンク付けされた状態で保存される。

【0054】次いで、IKE処理部11は、そのIPsec SAを、選択したIPsec処理装置であるIPsec処理装置12nに転送する(図4のステップS404)。

【0055】IKE処理部11からIPsec SA「SA₁₁」を受信したIPsec処理装置12nは(図5のステップS501)、そのIPsec SA「SA₁₁」を自らのローカルデータベース16に保存する(図5のステップS502)。

【0056】IPsec通信フェーズにおいては、IKE処理部11は対向するセキュリティゲートウェイ14からパケットを受信すると(図6のステップS601)、受信したパケットに基づいて、そのパケットを処理すべきIPsec SAをローカルデータベース15から検索する(図6のステップS602)。例えば、図3に示すように、ローカルデータベース15には、IPsec SA「SA₁₁」と、それに対応するIPsec処理装置の識別子「33」とが相互にリンク付けされた状態で保存されている。

【0057】次いで、IKE処理部11はエントリがあるか否かを判定する(図6のステップS603)。

【0058】エントリがある場合には(図6のステップS603のYES)、パケットを処理すべきIPsec処理装置を決定する(図6のステップS604)。例えば、パケットを処理すべきIPsec SAとしてIPsec SA「SA₁₁」が検索された場合には、そのIPsec SA「SA₁₁」に対応するIPsec処理装置として、識別子「33」で表されるIPsec処理装置が決定される。ここでは、識別子「33」で表されるIPsec処理装置はIPsec処理装置12nであるとする。

【0059】次いで、IKE処理部11は、パケットをIP in IP Tunnelingでカプセル化し、カプセル化したパケットをIPsec処理装置12nに対して転送する(図6のステップS605)。

【0060】一方、エントリがない場合には(図6のステップS603のNO)、受信したパケットを破棄し(図6のステップS606)、次のパケットの受信を待つ。

【0061】IPsec処理装置12nはIKE受信部11からパケットを受信すると(図7のステップS701)、カプセル化されたパケットを復元する、すなわち、パケットからカプセルを取り外す(図7のステップS702)。

【0062】次いで、IPsec処理装置12nは、ローカルデータベース16から、そのパケットに対応するIPsec SAを検索する(図7のステップS703)。

【0063】次いで、IPsec処理装置12nは、エントリが有るか否かを判定する(図7のステップS704)。

【0064】エントリが有る場合には(図7のステップS704のYES)、検索したIPsec SAに基づいて実際のIPsec処理(暗号化/復号及び認証)を

実行する(図7のステップS705)。

【0065】次いで、IPsec処理装置12nは、このようにしてIPsec処理したパケット19(図3参照)をネットワークへ送出する(図7のステップS706)。

【0066】一方、エントリがない場合には(図7のステップS704のNO)、受信したパケットを破棄し(図7のステップS707)、次のパケットの受信を待つ。

10 【0067】以上のように、本実施形態に係るセキュリティゲートウェイ装置によれば、次のような効果を得ることができる。

【0068】第一の効果は、処理負荷の高いIPsec処理からIPsec SA確立処理を分離させることにより、IPsec処理のスループットを上げることができる点である。

20 【0069】第二の効果は、IPsec処理部12を複数のIPsec処理装置12a-12nからなるクラスタ構成とすることにより、IPsec処理の負荷分散を図り、通信負荷に対して柔軟に対応することができ、スケーラビリティを確保することができる点である。

【0070】図8は、本発明の第2の実施形態に係るセキュリティゲートウェイ装置の構造を示す概略図である。

30 【0071】本実施形態に係るセキュリティゲートウェイ装置においては、第1の実施形態の場合と同様に、IKE処理部とIPsec処理部とはそれぞれ別のコンポーネントとして形成されているが、本実施形態におけるIKE処理部81とIPsec処理部82とはともにプロセッサ搭載ボードとして形成されており、内部バス83を介して相互に接続されている。これにより、IKE処理部81とIPsec処理部82とは外見上は単一の装置として構成されている。

【0072】IKE処理部81とIPsec処理部82を構成する複数のIPsec処理装置との間の通信は内部バス83を経由して行われる。

40 【0073】また、IKE処理部81とIPsec処理部82との間の通信路においては、データリンクレイヤの種別に応じて、転送方式を最適化することが可能である。

【0074】例えば、ATM(Asynchronous Transfer Mode:非同期転送モード)を用いる場合、IKE処理部81とIPsec処理部82との間をポイントツーポイント(Point to Point)の仮想チャネル(Virtual Channel:VC)で接続し、ダイレクトにLLC/SNAPカプセル化することにより、IP in IP Tunnelingのオーバーヘッドを軽減することができる。

50 【0075】

【発明の効果】以上のように、本発明に係るセキュリティゲートウェイ装置によれば、IPsec処理のスループットを上げることができるという効果を得ることができる。

【0076】本発明に係るセキュリティゲートウェイ装置においては、IPsec SA確立処理とIPsec処理とが分離されている。具体的には、認証キー交換手段（実施形態におけるIKE処理部）がIPsec SA確立処理、すなわち、IPセキュリティ通信に必要なパラメータをセキュリティゲートウェイとの間でネゴシエートする処理を行い、IPセキュリティ処理手段（実施形態におけるIPsec処理部）が認証キー交換手段から送られてきたパケットに対して実際にIPセキュリティ処理を実行する。このように、処理負荷の高いIPsec処理からIPsec SA確立処理を分離させることにより、IPsec処理のスループットを上げることが可能である。

【0077】また、IPsec処理部を複数のIPsec処理装置からなるクラスタ構成とすることにより、IPsec処理の負荷分散を図ることができ、高いスケラビリティを確保することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るセキュリティゲートウェイ装置のブロック図である。

【図2】IPsec SA確立フェーズにおける、第1の実施形態に係るセキュリティゲートウェイ装置の作動状態を示すブロック図である。

【図3】IPsec通信フェーズにおける、第1の実施形態に係るセキュリティゲートウェイ装置の作動状態を示すブロック図である。

【図4】第1の実施形態に係るセキュリティゲートウェイ*

*イ装置において、IPsec SA確立フェーズにおけるIKE処理部の動作を示すフローチャートである。

【図5】第1の実施形態に係るセキュリティゲートウェイ装置において、IPsec SA確立フェーズにおけるIPsec処理部の動作を示すフローチャートである。

【図6】第1の実施形態に係るセキュリティゲートウェイ装置において、IPsec通信フェーズにおけるIKE処理部の動作を示すフローチャートである。

【図7】第1の実施形態に係るセキュリティゲートウェイ装置において、IPsec通信フェーズにおけるIPsec処理部の動作を示すフローチャートである。

【図8】本発明の第1の実施形態に係るセキュリティゲートウェイ装置の概略図である。

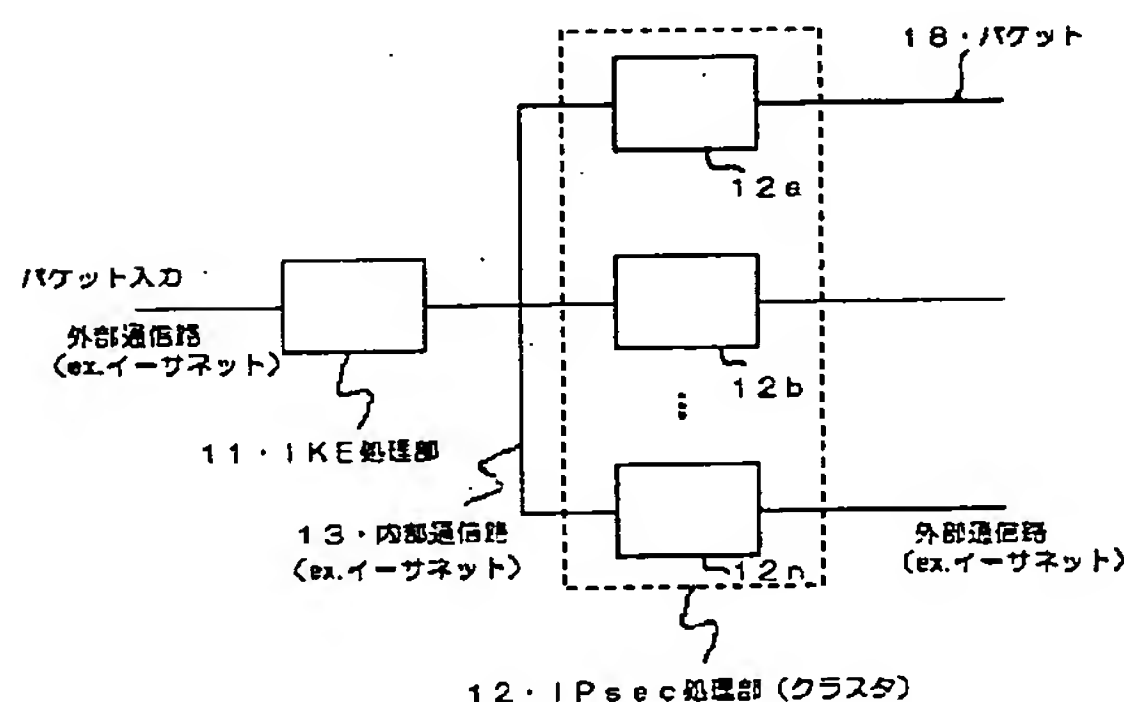
【図9】従来の信号通信システムの一例のブロック図である。

【図10】IPsecにおいて規定されているIP用セキュリティ認証ヘッダの一例を示す図である。

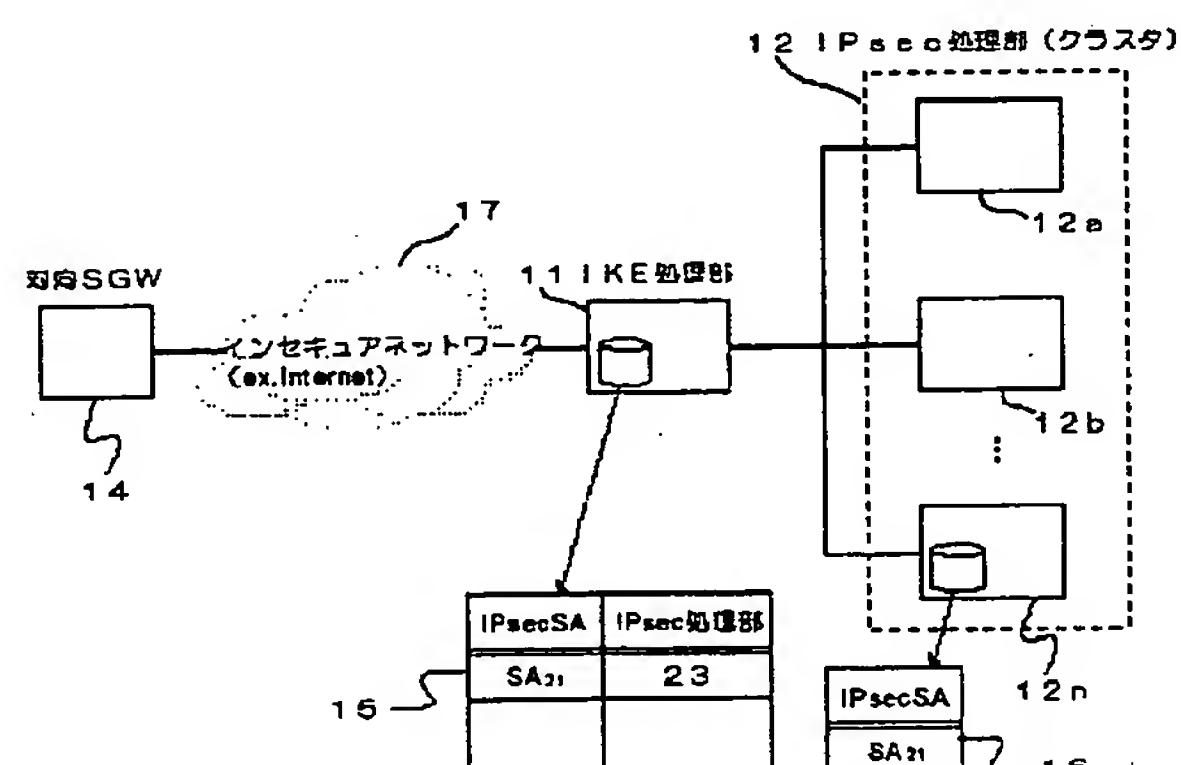
【符号の説明】

- 11 第1の実施形態におけるIKE処理部
- 12 第1の実施形態におけるIPsec処理部
- 12a-12n IPsec処理装置
- 13 内部通信路
- 14 セキュリティゲートウェイ
- 15 ローカルデータベース
- 16 ローカルデータベース
- 17 インセキュアネットワーク
- 18、19 パケット
- 81 第2の実施形態におけるIKE処理部
- 82 第2の実施形態におけるIPsec処理部
- 83 内部バス

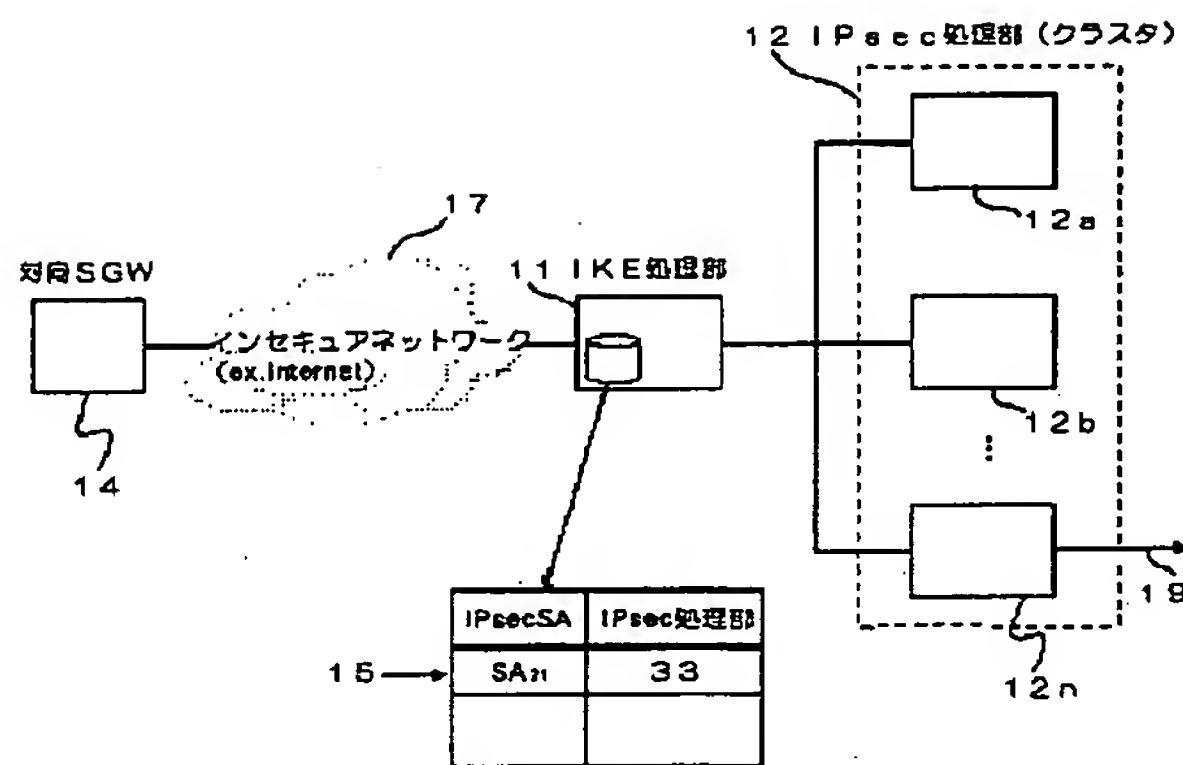
【図1】



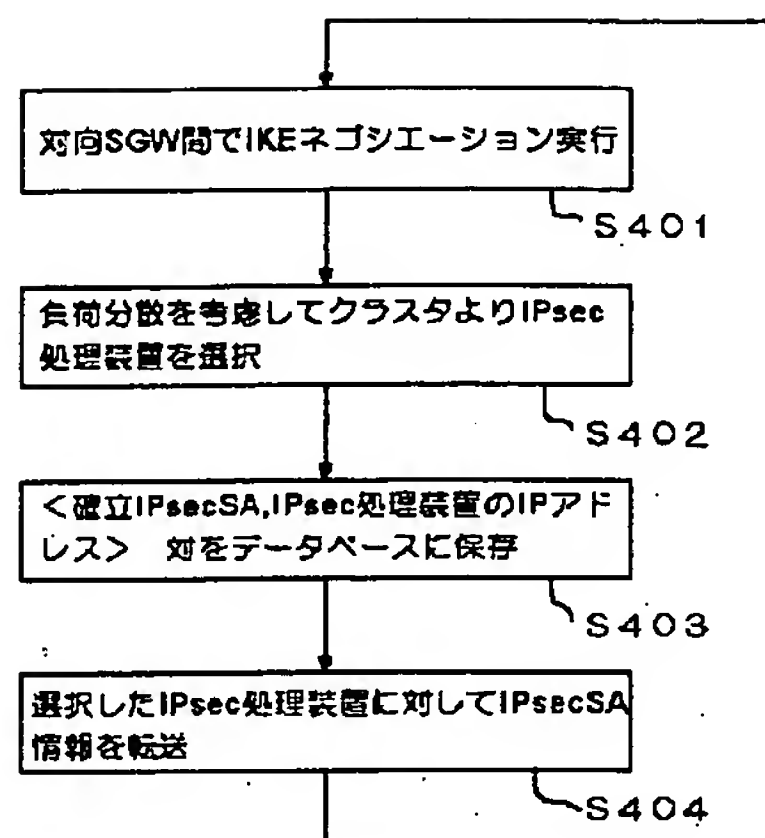
【図2】



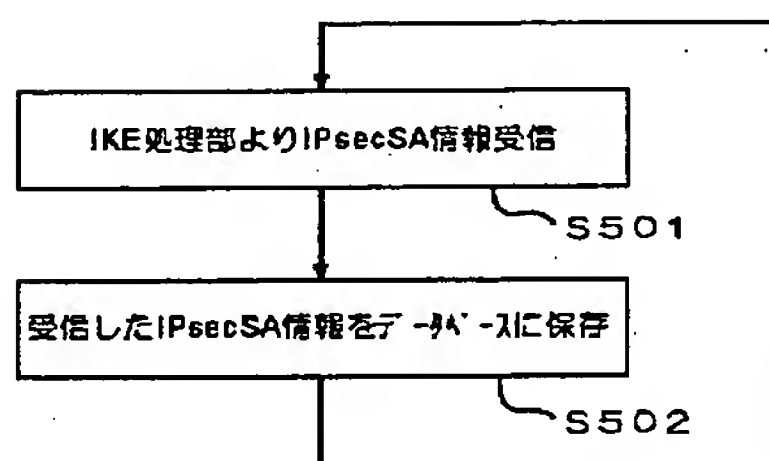
【図3】



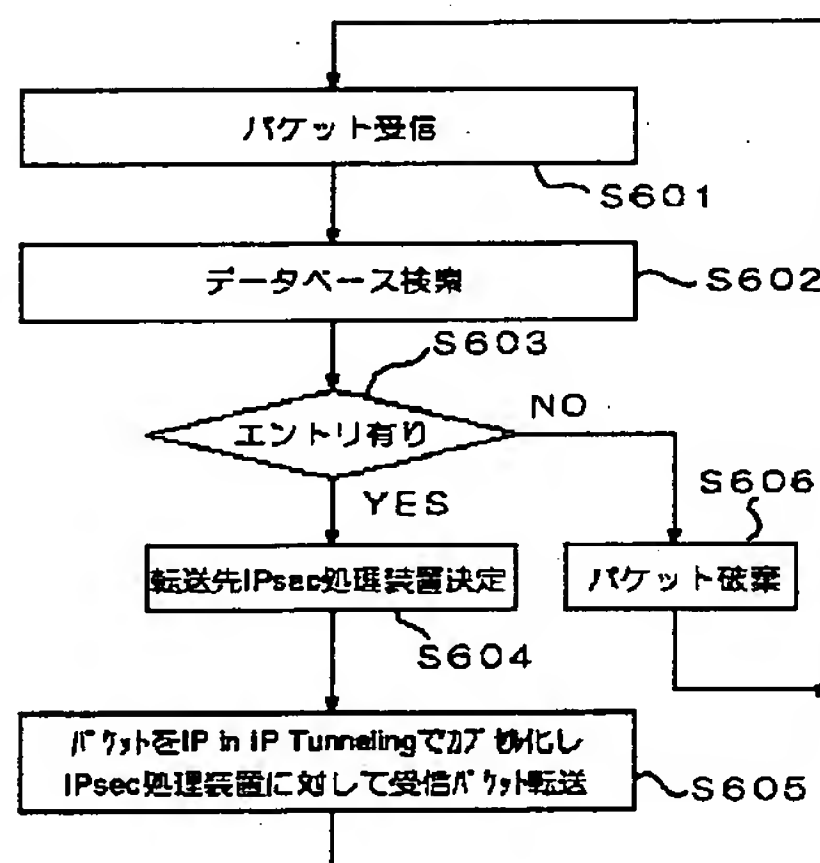
【図4】



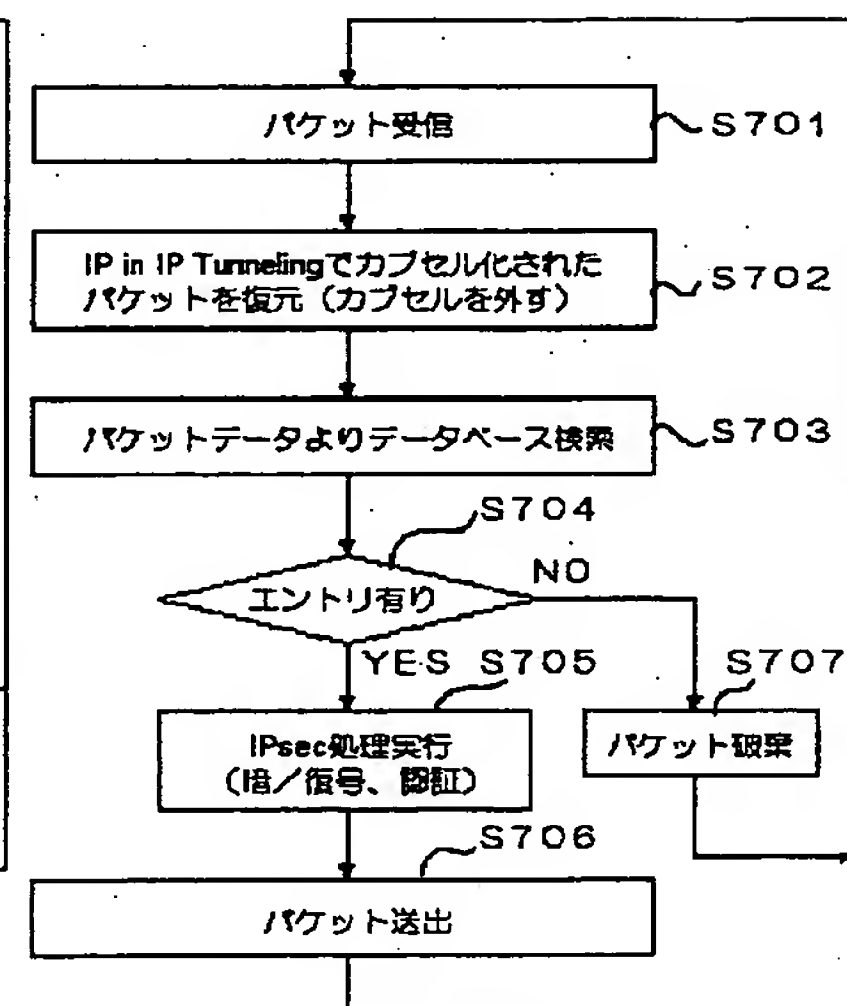
【図5】



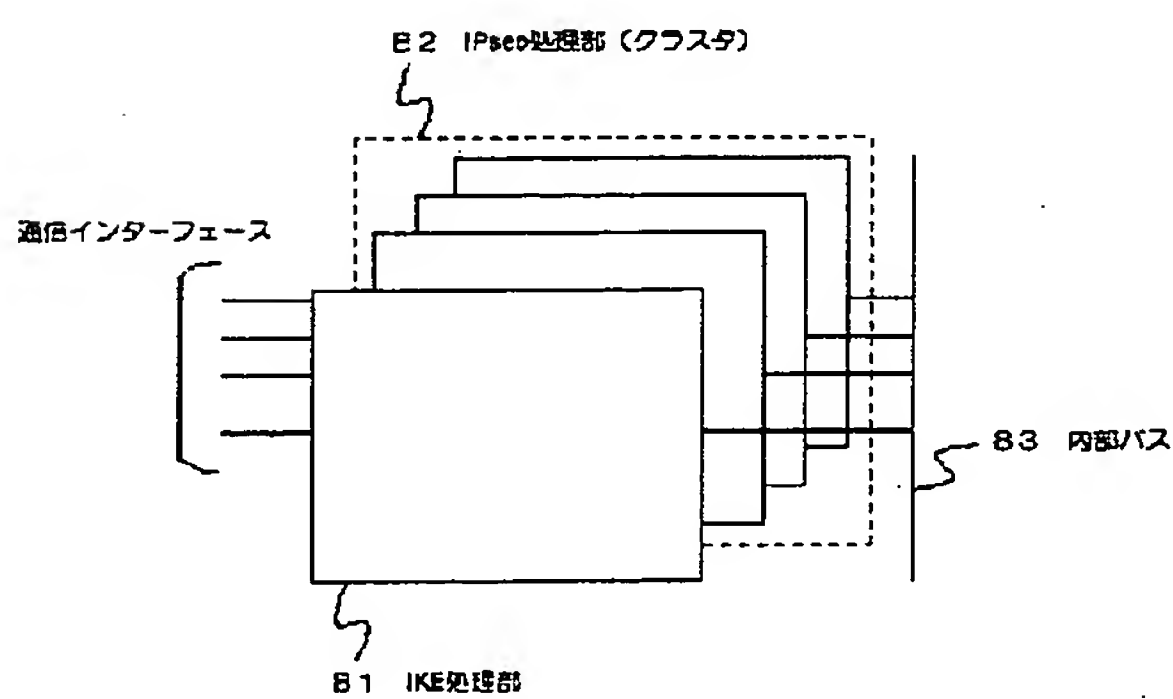
【図6】



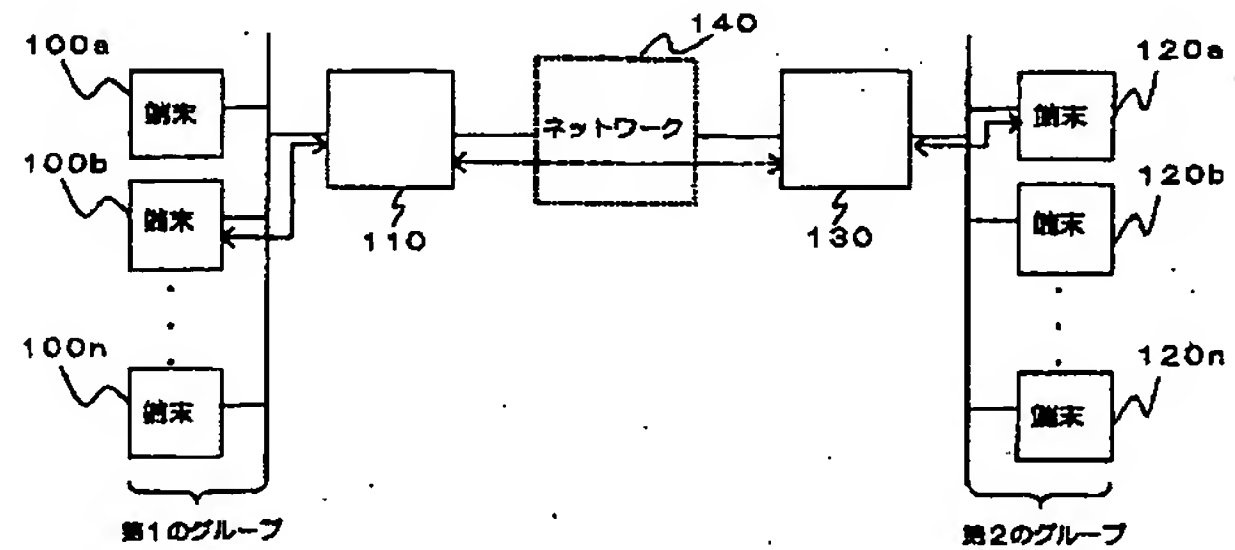
【図7】



【図8】



【図9】



【図10】

